CLAIMS

What is claimed is:

1. A method, comprising:

loading a virtual machine monitor (VMM) to support a plurality of virtual machines in a computer system, the VMM including a VMM multiplexer;

loading a first and a second virtual machine (VM) supported by the VMM; and

sharing a trusted hardware device between the first VM and the second VM using the VMM multiplexer.

2. The method of claim 1 wherein the VMM is loaded from firmware, the firmware including instructions compliant with an Extensible Firmware Interface (EFI) specification.

3. The method of claim 1 wherein sharing the trusted hardware device comprises multiplexing a first request from the first VM and a second request from the second VM to the trusted hardware device using the VMM multiplexer.

4. The method of claim 1, further comprising determining a first VM platform configuration and a second VM platform configuration.

5. The method of claim 4, further comprising:

determining a compound platform configuration based on a combination of the first VM platform configuration and the second VM platform configuration; and

storing the compound platform configuration in the trusted hardware device.

6. The method of claim 5 wherein the first VM platform configuration includes a first hash value based on information measured from the first VM and the second VM platform configuration includes a second hash value based on information measured from the second VM.

7. The method of claim 5, further comprising sealing secret information from the first VM with the compound platform configuration using the trusted hardware device.

8. The method of claim 7, further comprising unsealing the secret information using the trusted hardware device if a current first VM platform configuration matches the first VM platform configuration.

9. The method of claim 1, further comprising maintaining a queue of trusted hardware device requests by the VMM multiplexer, the trusted hardware requests sent to the trusted hardware device from the first VM and the second VM.

10. The method of claim 9, further comprising reporting a first request from the first VM is in progress when the trusted hardware device is polled by the first VM

regarding the status of the first request, the first request actually waiting in the queue to be processed by the trusted hardware device.

11. The method of claim 1 wherein the trusted hardware device includes a trusted platform module (TPM).

12. An article of manufacture comprising:

a machine-accessible medium including a plurality of instructions which when executed perform operations comprising:

loading a virtual machine monitor (VMM) in a computer system to support a first virtual machine (VM) and a second VM;

loading the first VM and the second VM; and

multiplexing a first trusted platform module (TPM) request received from the first VM and a second TPM request received from the second VM to a TPM of the computer system.

13. The article of manufacture of claim 12 wherein execution of the plurality of instructions further perform operations comprising:

receiving a first VM platform configuration from the first VM, the first VM platform configuration including information measured from the first VM;

computing a first virtual hash value based on the first VM platform configuration;

receiving a second VM platform configuration from the second VM, the second VM platform configuration including information measured from the second VM; and

computing a second virtual hash value based on the second VM platform configuration.

14. The article of manufacture of claim 13 wherein execution of the plurality of instructions further perform operations comprising sending the first virtual hash value and the second virtual hash value to the TPM, the TPM to compute a compound hash value based on the first virtual hash value and the second virtual hash value.

15. The article of manufacture of claim 14 wherein execution of the plurality of instructions further perform operations comprising sending a seal command to the TPM to seal secret information from the first VM with the compound hash value.

16. The article of manufacture of claim 15 wherein execution of the plurality of instructions further perform operations comprising sending an unseal command to the TPM from the first VM to unseal secret information associated with the first VM.

17. The article of manufacture of claim 12 wherein execution of the plurality of instructions further perform operations comprising maintaining a TPM request queue to queue a first TPM request from the first VM and a second TPM request from the second VM.

18. The article of manufacture of claim 17 wherein execution of the plurality of instructions further perform operations comprising reporting the second TPM request is in progress if the TPM is polled by the second VM, the second TPM request actually waiting in the TPM request queue.

19. A computer system, comprising:

a processor;

a trusted hardware device operatively coupled to the processor; and

at least one flash memory device operatively coupled to the processor, the at least one flash memory device including firmware instructions which when executed by the processor perform operations comprising:

loading a virtual machine monitor (VMM) in the computer system to support a first virtual machine (VM) and a second VM, the VMM including a VMM multiplexer;

loading the first VM and the second VM; and

multiplexing a first request from the first VM and a second request from the second VM to the trusted hardware device using the VMM multiplexer.

20. The computer system of claim 19 wherein execution of the plurality of firmware instructions further perform operations comprising:

maintaining a first VM platform configuration and a second VM platform configuration by the VMM multiplexer; and

storing a compound platform configuration based on a combination of the first VM platform configuration and the second VM platform configuration in the trusted hardware device.

21. The computer system of claim 19 wherein execution of the plurality of firmware instructions further perform operations comprising maintaining a queue of trusted hardware device requests by the VMM multiplexer, the trusted hardware device requests sent to the trusted hardware device from the first VM and the second VM.

22. The computer system of claim 19 wherein the firmware instructions compliant with an Extensible Firmware Interface (EFI) specification.

23. The computer system of claim 19 wherein the trusted hardware device comprises a trusted platform module (TPM).